



Telecom Management, Inc. d/b/a Pioneer Telephone  
39 Darling Avenue • South Portland • Maine • 04106  
Phone: (207) 774-9500 • Fax: (207) 774-9508  
[www.pioneertelephone.com](http://www.pioneertelephone.com)

Received & Inspected

FEB 29 2012

FCC Mail Room

Via Certified Mail, RRR, No. 7011 1570 0003 6409 6561

February 22, 2012

MARLENE H DORTCH  
OFFICE OF THE SECRETARY  
FEDERAL COMMUNICATIONS COMMISSION  
445 12<sup>TH</sup> ST SW  
STE TW-A325  
WASHINGTON DC 20554

Re: CPNI Compliance Certificate & Accompanying Statement  
Telecom Management, Inc. dba Pioneer Telephone (Pioneer)  
**EB Docket No. 06-36**

Dear Secretary Dortch:

I have enclosed a certificate and accompanying statement to comply with the requirements of 47 CFR §64.2009(e).

Please contact me at the telephone number listed above or via e-mail at [kphotiades@pioneertelephone.com](mailto:kphotiades@pioneertelephone.com) if you need additional information.

Sincerely,

Kevin Photiades  
Regulatory Manager

Encl.: 4 copies

cc: Best Copy and Printing, Inc. via e-mail to [FCC@BCPIWEB.COM](mailto:FCC@BCPIWEB.COM)

No. of Copies rec'd  
List ABCDE

0+4

**ANNUAL 47 CFR § 64.2009(e) COMPLIANCE CERTIFICATION**

**EB Docket 06-36**

*Received & Inspected*

*FEB 29 2012*

*FCC Mail Room*

Annual 64.2009(e) CPNI Certification for 2012 covering the prior calendar year 2011

Date Filed: February 22, 2012

Name of company covered by this certification: Telecom Management, Inc. d/b/a Pioneer Telephone

Form 499 Filer ID: 824332

Name of signatory: Peter Bouchard

Title of signatory: Chief Executive Officer


I, Peter Bouchard, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

  
Peter Bouchard

Attachments: Accompanying Statement explaining CPNI procedures

# **ANNUAL 47 CFR § 64.2009(e) COMPLIANCE STATEMENT**

**EB Docket 06-36**

**Received & Inspected**

**FEB 29 2012**

**FCC Mail Room**

Annual 64.2009(e) CPNI Statement for 2012

Name of Company: Telecom Management, Inc. d/b/a Pioneer Telephone

Form 499 Filer ID: 824332

This statement explains how Pioneer's operating procedures ensure compliance with the FCC's rules relating to CPNI.

Pioneer is a telecommunications service provider of landline-based local and long distance services and regards CPNI as information needing the greatest possible protection. Our customers' private data such as phone numbers called, length of phone calls, services purchased, and personal/credit card information is protected from dissemination to the public in a number of ways. Online access to customer accounts is password-protected and monitored electronically. Pioneer participates in VISA/Mastercard's compliance certification program on an ongoing basis – an independent third-party vendor scans our network for vulnerabilities and ensures Pioneer meets VISA/MC security standards. To keep hackers from accessing our network, Pioneer utilizes a perimeter-based firewall - SonicWall TZ 170 Unrestricted Node device - with ICSA Firewall 4.1, ICSA IPSec VPN 1.0d, and FIPS 140-2 industry certifications. In addition, real-time gateway anti-virus, anti-spyware, and intrusion prevention software such as Avast! is utilized to protect Pioneer from an array of network-based and sophisticated application layer threats. Finally, only explicit application-dependent communication ports are authorized for usage as part of our transportation layer security.

On the employee side, each employee of Pioneer is trained to understand the importance of keeping CPNI confidential and made to sign both a Confidentiality Agreement and a CPNI Policy Statement that includes information on how to recognize CPNI and protect it. Access to customer records is restricted only to those individuals whose jobs require such access. In addition, access to each customer account is tracked internally via the account software – each time the account is accessed, an electronic time and date stamp is recorded along with the name of the person who accessed the account. Employees are trained not to disclose CPNI to a customer over the phone unless the customer identifies certain unique information and provides their pre-established password. If the customer is requesting information that is too voluminous (e.g., copies of many month's worth of bills) to be relayed over the phone, the information is mailed to the customer's address of record.

In compliance with the FCC's rules, Pioneer monitors accounts and notifies its customers via e-mail and U.S.-mailed postcards when the following activity occurs: new online account set-up, password changes, address of record changes. The body of the e-mail / postcard states what activity has occurred and to contact Pioneer at our toll-free number immediately if the customer believes their CPNI was changed without their authorization.

If a breach of CPNI were to occur resulting in an unauthorized disclosure, Pioneer has put a plan in place to provide electronic, written and verbal notification of the breach to the US Secret Service, the FBI and the FCC.